NMCI Engineering Operations Procedure—GOVT Aide To Deploy

Release None

D407.1584.01
Final

Version 2.3

October 16, 2002

Enterprise Solutions

Navy Marine Corps Intranet

Change History

This document was based on the following form.

Forms Control			
Form Doc ID	**Version No.**	**Form Document Owner**	**Date**
DEV407	1.0	Document Management Center	

The following Change History Log contains a record of changes made to this document.

Published/ Revised Date	Version No.	Author(s) and Tech Lead Owner	Section Names/ Nature of Changes
October 16, 2002	2.3	Document Management Center	Made Final and converted to .pdf file
October 14, 2002	2.2	Document Management Center	Tracking number added. Edited for publication.
October 9, 2002	2.1.1	Laurie Esquivel	Modifications for ver 2.1
August 23, 2002	2.0	Laurie Esquivel	Modifications for ver 2.0
February 19, 2002	1.5	Laurie Esquivel	Added clarification to steps.
February 19, 2002	1.4	DMC	Added Doc Number, chart, edits.
February 11, 2002	1.3	Laurie Esquivel	Included Site Manager steps
February 4, 2002	1.2	Laurie Esquivel	Included Help Desk & Logistics steps
January 24, 2002	1.1	Laurie Esquivel	Included Pack up Kit procedures
January 16, 2002	1.0	Laurie Esquivel	First Draft

Contents

Figures

Figure **Page**

1 Introduction

The global nature of United States Navy and United States Marine Corps missions dictate the requirement for the worldwide deployment of both personnel and equipment. Both the Navy and Marine Corps operate and depend upon an extensive array of automation and telecommunications systems and networks to provide their deployed elements access to critical command and control, combat support, and combat service support information in voice, video and data formats. As specified in the Navy Marine Corps Intranet (NMCI) contract, the final NMCI architecture must ensure interoperability with and/or integration into these existing networks and systems.

With the introduction of NMCI on October 6, 2000, the concern of integrating NMCI deployables into non-NMCI environments assumed significant importance. Although NMCI is a services contract for both the Navy and Marine Corps, it is not designed to solve the integration issues of the heterogeneous environments that many deployable units face while in a deployable status. There are a vast number of sites, with varying heterogeneous environments, which will have to interoperate with deployable seats provided by NMCI. The employment of deployable seats requires the interface between NMCI and the Navy's Integrated Shipboard Network System (ISNS), formally called Information Technology for the 21st Century (IT-21), and the Marine Corps Tactical Network (MCTN). ISNS supports all Navy and Marine personnel while afloat or pierside, while the MCTN supports Marine Expeditionary Force (MEF) and other Marine Corps elements in a tactical environment.

The major interoperability issue affecting NMCI deployables solutions is with those networks that provide access to the NIPRNET/SIPRNET but as of yet, do not have a trusted relationship with the NMCI environment. Essentially this includes all networks outside the responsibility of NMCI, and those not transitioned, specifically ISNS, MCTN, and Joint Service tactical networks established by a Joint Task Force in a theater of operations. Navy and Marine Corps units must also operate in fully deployed, non-shipboard environments as well as at CONUS and OCONUS locations without NMCI services and connectivity during training events. Lastly, units that must deploy directly to ships at sea or pre-established ashore networks cannot depend on the transmission of their unit data over the limited tactical bandwidth available to that location. The NMCI Deployables Support Plan (DSP) addresses all of these operational scenarios.

This document describes the steps required to move accounts and machines out of and into the NMCI network.

1.1 Audience

The intended audience of this document is primarily, but not limited to, Navy and Marine Corps IT Representatives, Deployable Users, and those who have a need to understand the technologies used in service delivery and the ongoing support of the NMCI Deployables. A basic understanding of computers, networks, NMCI, e-mail routing, DNS, and the former NMCI Navy and USMC deployment methodology, would be of significant help while reading this document. It may also be helpful for those wishing to gain an overall understanding of how a NMCI deployable seat will deploy and re-integrate into the NMCI environment.

1.2 Scope

The NMCI deployable process will allow users to receive electronic mail (e-mail) and access user's data through data migration, and will provide limited access to NMCI services while in a deployed status. Seats will still be functional via a local unit-level LAN (whether in a training or real world scenario event) from the theater of deployment or in a stand-alone mode. The post-deployment process addresses the necessary steps involved with reinstating the seat and user account into direct connectivity within the NMCI environment after the deployment.

2 Aide To Deploy/Return Overview

The intention of the deployable process is to provide the operational unit the ability to achieve and sustain self-sufficiency in all facets while in a deployed status.

To achieve and sustain self-sufficiency, it is highly recommended and encouraged for the Commanding Officer of the deploying unit and the designated Unit IT representative to ensure that all configuration management and configuration control processes and precautions are taken and followed. Documenting and noting all configuration changes made to each NMCI deployable seat for integration into the deployed location's network will facilitate a quick and seamless reintegration into the NMCI environment upon return from the deployment.

The following is provided as information that will be useful for Unit IT's to become familiar with and understand the overall steps/processes involved when a User Account or Machine is transitioned to a Deployed or Returning status.

2.1 Data Management

During deployment, data and user profiles may exist in areas that are not accessible once deployed from NMCI standards. It is important to move all data to a location a user can easily find and access. The following bullets may help with this operation:

- Changing Domains causes new profiles to be generated. User profiles contain My Documents, Favorites, and application configuration information. In most cases simply moving the contents of "My Documents" from the NMCI user profile to another accessible location will solve this issue (i.e. "C:\username").
    - Logon as the NMCI user; open Windows Explorer and navigate to the **My Documents** folder. This folder houses all files associated with the user. Search for *.doc, *.xls and other file extensions containing user data. Select all pertinent data files and copy.
    - Navigate to a known and accessible location (i.e. "C:\"), create a new folder and copy the user data files into the new folder.
    - Perform these actions for all user profiles where necessary.
- E-mail data that has been stored in the default NMCI Exchange will not be accessible once deployed. The availability of this mail will depend on the user creating (if not already in use) a personal folder (*.pst) and coping the desired e-mails to that folder. This folder, which exists as a .pst file, must be stored in the location created in the previous step.

  - Open **Microsoft Outlook** and select from the File menu – **File – New – Personal Folder File** (.pst) and create a new Personal Folders File.
  - Save the file name to a location the user can reach when deployed (see previous data management section for file location).
  - Name the Outlook folder, select **Compressible Encryption**, and assign a password. Do not save the password in a password list.
  - The folder then shows up in the Outlook Folder view where e-mail can be moved then later opened using Outlook under the NMCI user account or the deployed user account if mapped properly.

2.2 Deploying From NMCI

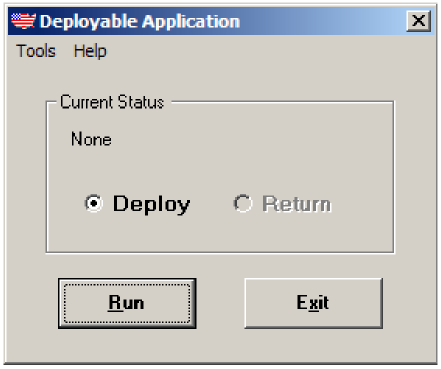
Deploying an NMCI seat or user from the NMCI environment to an external network requires the following general steps:

2.2.1 Step 1: Notifying ISF

- Unit IT provides list of machines and users that will be deployed to the CTR. List must include NMCI Asset Tag #, and NMCI User Account name. Unit IT indicates their Exercise Level (Local, CONUS, OCONUS, or Extended).
- CTR enters machine and user names into eServices. If eServices is unavailable to CTR, then e-mail the list to NMCI Help Desk. CTR identifies POC and phone number for each Command and identifies Exercise Level to Help Desk.
- NMCI Help Desk receives request and:
  - Ensures users are in the “Deployable” security group.
  - Ensures Unit IT POC is in the “Unit IT Rep” security group.
  - Ensures machine is in the “Deployable” software group.
  - Opens Remedy ticket for Pack Up Kit (PUK) creation and tracking. Ticket is submitted to Queue Manager of Unit site.
- Queue Manager follows PUK Standard Operating Procedures (SOP) for consolidation and delivery.
- Unit IT receives PUK and signs for the shipment. Unit IT inventories and verifies the packing list. If a discrepancy exists, the Unit IT notifies NMCI Help Desk.
- Queue Manager closes ticket.

2.2.2 Step 2: Machine And User Account Deployment

- At the time of deployment, the application will be on the user's seat. The user will launch the Deployable Seat Application by going to **Start** > **Program Files** > **Deployable Seat Application** and select the **Deployable Seat Application**. The following status screen is displayed.



Current Status

None

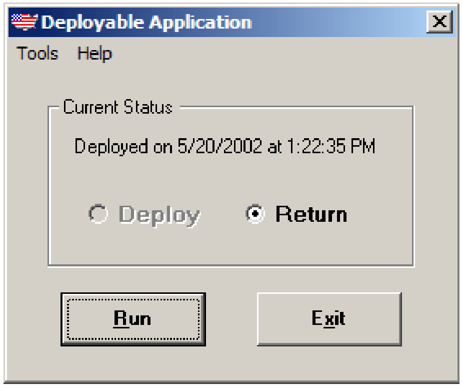
● Deploy ○ Return

Figure 1—Deployable Application

Note: Before a user deploys the machine, you can click on the **Tools** drop down menu and select the **Service Check** item to ensure all services are functioning properly. Select **OK** to continue.

- To Deploy the Workstation, click the **<u>R</u>un** button. A status bar will appear displaying how far the application has progressed. When complete, select the **OK** button.

- The Deployable Application will now show the status of the machine as being deployed and indicate the last date and time the machine was deployed.



Current Status

Deployed on 5/20/2002 at 1:22:35 PM

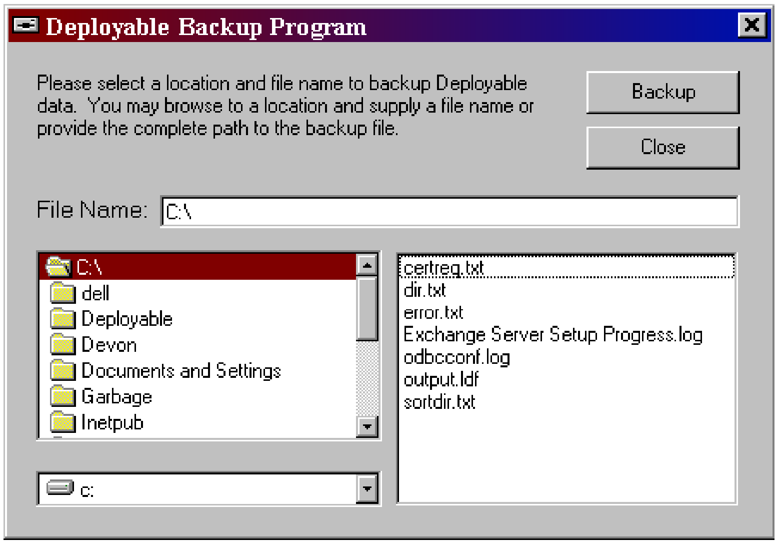
○ Deploy ● Return

Figure 2—Current Status

- If at any time the application fails or generates an unexpected message, the Unit IT will notify the NMCI Help Desk (866-THE-NMCI).

- The user should now select the **Tools** drop down menu and select the **Backup** item. This will backup the deployable configuration information critical to the Deployable process, in case the Deployable application needs to be reinstalled while on deployment. The following screen will be displayed, prompting for a backup location (CD-ROM or Floppy is recommended).

Note: The location where the file will be saved must be present in the “File Name” text box (i.e. “A:\filename”).



Deployable Backup Program

Please select a location and file name to backup Deployable data. You may browse to a location and supply a file name or provide the complete path to the backup file.

File Name: C:\

Figure 3—Deployable Backup Program

- Select the location, type a file name and click on the **Backup** button. When complete, select **OK** and then **Close**.
- Select **Exit** to complete the process.
- A user’s e-mail account can be redirected at anytime. To start, stop, or change the e-mail redirection, go to the following website https://deployables2/. If user does not have access to the NMCI network, he/she may call or e-mail the NMCI Help Desk to initiate the redirection.
- The machine is now ready to be disconnected from the NMCI environment. You should shutdown, and once the machine has been turned off, disconnect it.
- If any errors were encountered during the above process, contact the NMCI Help Desk for assistance (866-THE-NMCI).

2.2.3 Configuration Information

- Unit IT should maintain listing of NMCI Assets and users. Listing should contain Asset Tag #, Computer Name, NMCI Domain Name, Network Settings (TCP/IP, Proxy Settings, NIC Settings) user name, NMCI user IDs, and NMCI applications. This information may be required during reintegration into the NMCI network.

- Unit IT must create a Timestep VPN configuration disk to be used in case a machine requires a rebuild. To create the VPN Configuration Disk:
  - Go to **Start** > **Programs** > **TimeStep > Permit Client > PERMIT/Client for Windows 2000**.
  - Press the **Save to File** button. Choose the path (presumably a floppy) and filename for the exported profile and save it.

2.3 Deployed Operational Support

2.3.1 Maintenance

In instances where a hardware problem is encountered while deployed, the unit can do one of two things:

- Resolve the problem internally (replace with spare part, spare system or re-install software with supplies provided in the PUK).

Or

- Unit IT calls or e-mails the NMCI Help Desk for assistance.

2.3.2 Refreshing The Pack-Up Kit While Deployed Or Replacing Failed Unit

- Unit IT notifies the Help Desk of spares re-supply or replacement requirements and specifies delivery location.
- Immediately upon receipt of the notification, the Help Desk will open a ticket and send to Queue Manager at Unit home site.
- Immediately upon receipt of the Help Desk ticket, the Queue Manager follows PUK SOP for consolidation and expedient delivery.
- Unit IT receives PUK and signs for the shipment. Unit IT inventories and verifies the packing list against the order.
- Queue Manager closes ticket.

2.3.3 Reimaging A Machine While In A Deployed Status

Using NMCI Gold Client Build installation manual, Build Diskette, and CD-ROMs, follow instructions in the Appendices based on type of machine you are reimaging. Unit IT will need the NMCI Assets and users list to complete the reimaging procedure. Listing should contain Asset Tag #, Computer Name, NMCI Domain Name, Network Settings (TCP/IP, Proxy Settings, NIC Settings) user name, NMCI user IDs, and NMCI applications.

2.3.3.1 APPENDIX C – DELL PORTABLE STAGING

- Go to **Appendix C** of the **NMCI Gold Client Build Bundle**.
- Go to **Dell Portable CD-ROM Installation Section**.
- Gather items under **Requirements Section**. (You do not need the Docking station.)
- Follow **Part One**.

Note: If machine does not boot from Floppy, check the following:

- Check BIOS is set to boot from floppy. To enter BIOS:

  1. Power ON machine.
  2. During power-on memory test, press **F2**.
  3. Press **Alt-P** until the **Boot Order** screen appears.
  4. Follow the on-screen instructions to set the boot order.
  5. Set 1st Boot Device to **Diskette Drive**.
  6. Set 2nd Boot Device to **Internal HDD**.
  7. Set 3rd Boot Device to **CD/DVD/CD-RW Drive**.
  8. Press **Esc** to exit.
  9. Select **Yes** to save changes and reboot.

  If floppy does not boot:

  1. Put floppy in functioning NMCI Client.
  2. Click **Start > Run** and type **C:\DOS\XBOOT F**.
  3. Click **OK**.

- Follow **Part Two**

Note: Computer Name must be the original name of the NMCI machine when you return to NMCI.

Note: Administrator password should be reset to the “xdeployadmin” password.

Follow the instructions based on the type of network connection you will be utilizing. Options are:

- **Workgroup Section** (steps 1-4) or
- **Join a Domain Section** (steps 1-4).

  - **Join Computer to [site specific] Domain Screen Section** (steps 1 – 3).
  - **Network Settings Screen Section** (steps 1 – 2).
- Follow **Completing the Windows 2000 Setup Wizard Screen Section** (steps 1 – 9).

2.3.3.2 APPENDIX D – DOLCH FLEXPAC STAGING

- Go to **Appendix D** of the **NMCI Gold Client Build Bundle**.
- Go to **Dolch FlexPac CD-ROM Installation Section**.
- Gather items under **Requirements Section**. (You do not need the Docking station.)
- Follow **Part One**.

Note: If machine does not boot from Floppy, check the following:

- Check BIOS is set to boot from floppy. To enter BIOS:
  1. Power ON machine.
  2. During power-on memory test, press **Delete**.
  3. Navigate to **Advanced BIOS Features**, select and press **Enter**.
  4. Follow the on-screen instructions to set the boot order.
  5. Set 1st Boot Device to **Diskette Drive**.
  6. Set 2nd Boot Device to **Internal HDD**.
  7. Set 3rd Boot Device to **CD/DVD/CD-RW Drive**.
  8. Press **F10** to save changes.
  9. Press **Enter** to reboot.

If floppy does not boot:

1. Put floppy in functioning NMCI Client.
2. Click **Start > Run** and type **C:\DOS\XBOOT F**.
3. Click **OK**.

- Follow **Part Two**

Note: Computer Name must be the original name of the NMCI machine when you return to NMCI.

Note: Administrator password should be reset to the "xdeployadmin" password.

Follow the instructions based on the type of network connection you will be utilizing. Options are:

- **Workgroup Section** (steps 1-4) or
- **Join a Domain Section** (steps 1-4).
    - **Join Computer to [site specific] Domain Screen Section** (steps 1 – 3).
    - **Network Settings Screen Section** (steps 1 – 2).
- Follow **Completing the Windows 2000 Setup Wizard Screen Section** (steps 1 – 9).

2.3.3.3 APPENDIX E – DOLCH NOTEPAC STAGING

- Go to **Appendix E** of the **NMCI Gold Client Build Bundle**.
- Go to **Dolch Notepac CD-ROM Installation Section**.
- Gather items under **Requirements Section**.
- Follow **Part One**.

Note: If machine does not boot from Floppy, check the following:

- Check BIOS is set to boot from floppy. To enter BIOS:
    1. Power ON machine.
    2. During power-on memory test, press **F2**.
    3. Press the side arrow keys "←/→" until the **Main** screen appears.
    4. Press the up/down arrow keys "↑/↓" until the **Boot Sequence** screen appears.
    5. Press **Enter** and follow the on-screen instructions to the boot order.
    6. Set 1st Boot Device to **Diskette Drive**.
    7. Set 2nd Boot Device to **Internal HDD**.
    8. Set 3rd Boot Device to **CD/DVD/CD-RW Drive**.
    9. Use the arrow key "→" to select **Exit**.
    10. Press the up/down arrow keys "↑/↓" to select **Save Changes and Exit**.
    11. Press **Enter** twice to save changes and reboot.

If floppy does not boot:

1. Put floppy in functioning NMCI Client.
2. Click **Start > Run** and type **C:\DOS\XBOOT F**.
3. Click **OK**.

- Follow **Part Two**

Note: Computer Name must be the original name of the NMCI machine when you return to NMCI.

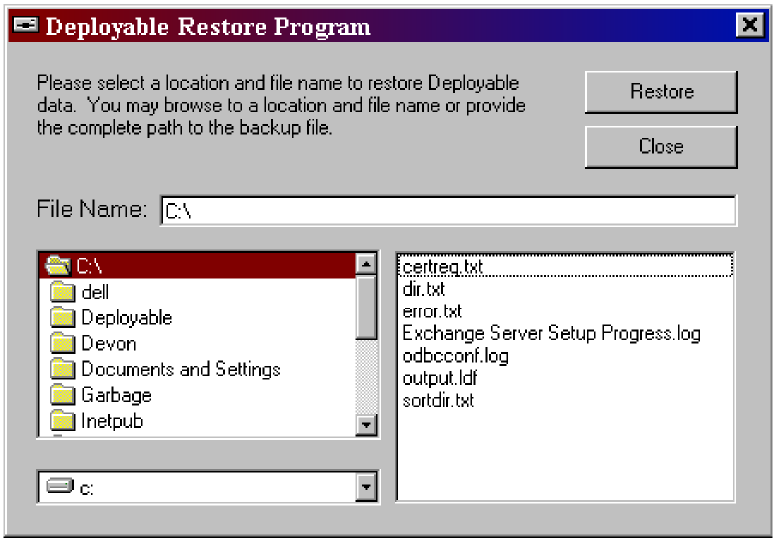
Note: Administrator password should be reset to the "xdeployadmin" password.

Follow the instructions based on the type of network connection you will be utilizing. Options are:

- **Workgroup Section** (steps 1-4) or
- **Join a Domain Section** (steps 1-4).
  - **Join Computer to [site specific] Domain Screen Section** (steps 1 – 3).
  - **Network Settings Screen Section** (steps 1 – 2).
- Follow **Completing the Windows 2000 Setup Wizard Screen Section** (steps 1 – 9).

Once the machine has been reloaded with the Gold Client Image, you need to reload the Deployable Application by following the steps below:

- Login using the administrator account and password you assigned above.
- Install the Deployable Seat Application Program from the CD-ROM or floppy by running **\Components\Client\Deploy\install.exe** on the CD-ROM or **\install.exe** from the floppy.
- Launch the Deployable Seat Application by going to **Start** > **Program Files** > **Deployable Seat Application** and select the **Deployable Seat Application**. Select the **Tools** drop down menu. Click on the **Restore** option and the following screen will appear. Navigate to where you saved the backup file and highlight the file, then select the **Restore** button. Select **OK** when complete.



Deployable Restore Program

Please select a location and file name to restore Deployable data. You may browse to a location and file name or provide the complete path to the backup file.

File Name: C:\

```
C:\
dell
Deployable
Devon
Documents and Settings
Garbage
Inetpub
```

```
certreq.txt
dir.txt
error.txt
Exchange Server Setup Progress.log
odbcconf.log
output.ldf
sortdir.txt
```

c:

Figure 4—Deployable Restore Program

- Once the configuration files are restored, select the **Close** button, and then select the **Exit** button.
- To install Norton Anti Virus: Go to **Start** > **Run**, type in **c:\winnt\custom\nav\setup.exe** and press **Enter**. Select the default settings during the install.
- To install PAL Software (required if you want to RAS into NMCI prior to returning):

Note: You must have your PKI Cert on diskette to RAS and load both the PAL and VPN software.

  - Insert the VPNINST CD.
  - Copy the **d:\pallv411-nmci** folder to the **c:\winnt\custom** folder.
  - Go to **Start > Run** and type in **c:\winnt\custom\pallv411-nmci\pal3disk\disk1\setup.exe**.
  - Select the default settings during install.
  - Copy the **\Scripts** subdirectory from either the VPNINST cdrom or VPNINST Script floppy disk to the **c:\program files\PAL** subdirectory. This will overwrite the existing Scripts subdirectory.
  - Create a generic local user account.
  - Select **OK** to reboot the machine.

Note: To configure the PAL software *** YOU MUST LOGIN WITH A "USER" ACCOUNT, NOT AN ADMINISTRATOR ACCOUNT, OTHERWISE APPLICATION

WILL ONLY BE AVAILABLE TO ACCOUNTS WITH ADMINISTRATIVE PRIVLIDGES. **

- Login with the above created user account.
- Double-click the **PAL** icon on the desktop.
- Click **Continue**.
- Click **OK** to Close PAL help.
- Type User's login ID under Name for Login Sequence.
- Select **NMCI Connect** under Template.
- Select **OK**.
- Click the **Name Search** button.
- Type in your City and select **OK**.
- At user ID connection screen, enter the users logon name into the "Host User ID" box.
- Under "Host Realm", enter **nawesdnivp99.nadsuswe.nads.navy.mil**.
- Ensure the boxes are checked next to "Host User ID" and "Host Realm" then click **DONE**.
- Click **CLOSE**.
- Logout and login as an administrator account to continue software installs.

- To install VPN Software (required if you want to RAS into NMCI prior to returning):

Note: You must have your PKI Cert on diskette to RAS and load both the PAL and VPN software. You must have the diskette you created with the TimeStep VPN configuration load.

- Insert the VPNINST CD.
- Copy the **d:\vpninst** folder to the **c:\winnt\custom** folder.
- Go to **Start** > **Run** and type in **c:\winnt\custom\vpninst\setup.exe**.
- Select the default settings during install.
- Create a subdirectory under *c:\program files\timestep* called Cert and copy the users DoD PKI certificate into that subdirectory.
- Go to **Start** > **Programs** > **TimeStep > Permit Client > PERMIT/Client for Windows 2000**.

- Insert the TimeStep VPN configuration disk.
- Press the **Load from File** button. Choose the path (presumably a floppy) and filename for the exported profile and select **OK**.
- Select the Modem and select **OK**.
- Right click on the **PKI VPN Gateway** folder under the Profile List and click **Set the Active Profile**.
- Right click on the Red "**T**" in the icon tray and deselect the **Login at Startup** option.
- Reboot the machine.

- You may now reload any Legacy Applications this machine requires by following the Central Design Authority (CDA) instructions for those applications.
- If you need to join the machine to a non-NMCI Domain, follow the local guidelines for your specific location.

2.3.4 Prior To Returning

- To cancel user e-mail redirection, prior to returning and plugging into the NMCI network, the user can either call the NMCI Help Desk and ask to have their e-mail account redirection terminated or changed, or they can RAS/VPN to https://deployables2/ and select **Stop Redirection**. E-mail will stop being redirected and stay in NMCI e-mail account. If user does not have access to the NMCI network, he/she may call or e-mail the NMCI Help Desk to change the redirection status.

Note: This step must be completed prior to departing the deployed network environment, so no e-mails will be lost during the transit period.

2.3.5 Data Management

During deployment, data and user profiles may exist in areas that are not accessible once returned back to NMCI standards. It is important to move all data to a location a user can easily find and access the data. The following bullets may help with this operation:

- Changing Domains causes new profiles to be generated. User profiles contain My Documents, Favorites, and application configuration information. In most cases simply moving the contents of My Documents from the Deployed user profile to NMCI user profile.
  - Logon as the supplied local administrative account, open Windows Explorer and navigate to the **C:\Documents and Settings** folder. This folder houses all user profiles, locate user profiles associated with the

deployed Domain and search for *.doc, *.xls and other file extensions containing user data. Select all pertinent data files and copy.

- Navigate to the NMCI User profile and locate the desktop folder. Create a new folder in the Desktop folder and copy the user data files into the new folder.
- Perform these actions for all user profiles where necessary.

- E-mail data that has been redirected to alternate locations will not be accessible once returned to NMCI. The availability of this mail greatly depends on the e-mail client and configuration. If Microsoft Outlook is used as the remote e-mail client, the following provides a method of saving e-mail for later accessibility. Please note this operation should be performed prior to disconnecting from the deployed e-mail location, unless Off Line Folders were configured, e-mail is not available, and must be done under the user's account/credentials.
  - Open Microsoft Outlook and select from the File menu – **File – New – Outlook Data File** and create a new Personal Folders File.
  - Save the file name to a location the user can reach when using their NMCI account. (See previous data management section for file location.)
  - Name the Outlook folder, select **Compressible Encryption** and assign a password. Do not save the password in a password list.
  - The folder then shows up in the Outlook Folder view where e-mail can be moved, then later opened using Outlook under the NMCI user account.

2.4 Returning To NMCI

Returning an NMCI seat or user account from an external network to the NMCI environment requires the following general steps:

2.4.1 Step 1: Notifying ISF

- Unit IT provides list of machines and users that will be "Returning" to the CTR. List must include NMCI Asset Tag #, and NMCI User Account name.
- CTR enters machine and user names into eServices. If eServices is unavailable to CTR, then e-mails the list to the NMCI Help Desk.
- NMCI Help Desk receives request:
  - Help Desk creates ticket and sends to Queue Manager at Unit home site.
- Queue Manager coordinates with Unit IT to have all spares picked up within 2 weeks of unit termination of deployment status (reintegration of seats into NMCI).

- Queue Manager closes ticket.

2.4.2 Step 2: Returning The Machine

- Changing Domains: If you changed Domains during deployment you must follow these steps to successfully reintegrate:
    - Plug into NMCI Network.
    - Unit IT logs in as the local machine administrator.
    - Validate the TCP/IP settings, Proxy Server settings and other network configurations are set to NMCI Enterprise standards. Refer to the listing of NMCI Assets and users created upon deployment.
    - Join the NMCI Domain.
        - Right click on **My Computer**.
        - Select **Properties**.
        - Select **Network Identification** tab.
        - Select **Properties**.
            - Verify the Full Computer Name is: "computername.FullyQualifiedDomainName"

              i.e.: wllemrtest01.nadsusxx.nads.navy.mil
            - If not, select the **More** button.
                - Type in Fully Qualified Domain Name under Primary DNS Suffix.

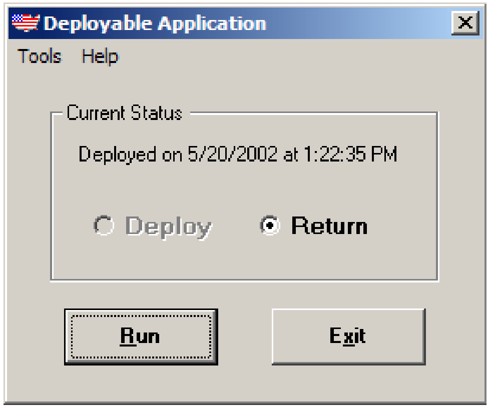
            Note: FQDN for machines NADSUSWE domain is **nadsuswe.nads.navy.mil**

            - Select **OK**.
        - Select radio button for **Domain**.
        - Type in Fully Qualified Domain Name.
        - Select **OK**.
            - When prompted for an account and password provide the Unit IT NMCI account name and password.
        - Select **OK** three times and reboot machine when prompted.

Note: It is the responsibility of the unit IT to completely remove any software that was installed during deployment, before reintegrating into the NMCI environment.

Uninstalling applications requires logging in under a local administrative account (xDeployAdmin). However, once you rejoin the NMCI domain, the admin account will be renamed to xadministrator, utilizing the password created during Gold Disk reimage.

- User should now login to machine and proceed with return instructions.
- Once the machine is connected to the NMCI network, the user runs the Deployable Application Process by going to **Start** > **Program Files** > **Deployable Seat Application** and select the **Deployable Seat Application**. The following screen will appear indicating when the machine was deployed out of the NMCI environment:



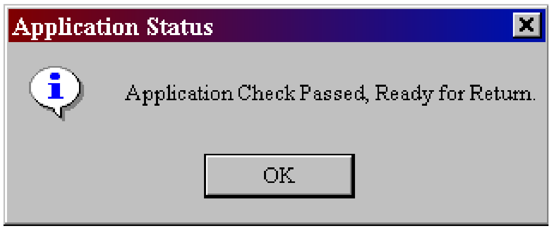
Current Status

Deployed on 5/20/2002 at 1:22:35 PM

○ Deploy ● Return

Figure 5—Current Status

- Select the **Tools** drop down menu and choose the **Application Check** item. If no un-subscribed applications remain loaded on the machine, the following status will be displayed:

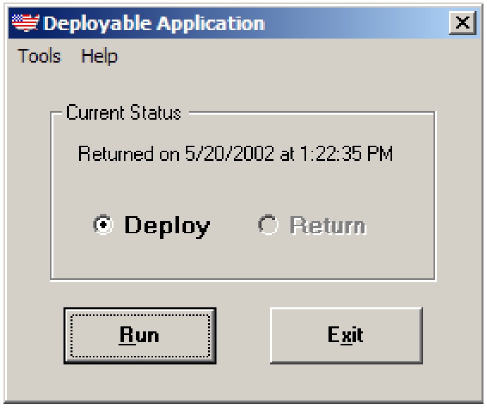


Application Check Passed, Ready for Return.

Figure 6—Application Status

- If applications that were installed during deployment remain on the computer, they must be removed prior to returning to the NMCI environment. Continue removing until the above status is displayed. (Uninstalling applications requires the use of the xDeployAdmin Account.)

- Once the machine indicates it is ready for return, select the **OK** button. At this point, select the **Run** button on the Deployable Application process. A status bar will appear displaying how far the application has progressed. When complete, select the **OK** button, and the following screen is displayed indicating a successful return:



Current Status

Returned on 5/20/2002 at 1:22:35 PM

● Deploy ○ Return

Figure 7—Deployable Application (Deploy)

- Select the **Exit** button to complete the process and reboot machine.

Note: If you reimaged the machine you must now call the NMCI Help Desk and tell them you have returned a Deployed Machine that has been re-imaged and you need a Radia connect to reload NMCI Enterprise applications. The Help Desk will create a ticket and assign it to the Software Distribution Group. They will contact the user and schedule a Radia connect. You will skip this step if machine was not reimaged.

- A user can start, stop, or change the e-mail redirection. Go to the following website https://deployables2/.

3 Troubleshooting Aids

Refer to the Deployable Solutions Plan (DSP) APPENDIX D: NMCI Seat and User Account Reintegration Checklist for key areas to review when attempting to return to the NMCI environment. Viewing the proper settings on an NMCI machine that has successfully returned to the NMCI environment can validate the settings.

If the Unit IT is unable to resolve issues, they should contact the ISF Help Desk at (866) 843-6624 (THE-NMCI).